Personal Electronic Devices, Photographs and Images

Key learning from Serious Case Review: Nursery Z which informs the approach

The Serious Case Review into Nursery Z, where personal devices were a tool used by the perpetrator to abuse and share images, found;

"One tangible lesson that has come out from this review has been the danger of mobile phones within [education] settings."

"Challenge inappropriate behaviour such as use of mobile phones."

What are personal devices?

Personal devices are devices owned by the individual, **not** the setting.

- Personal devices can be, but are not limited to;
  - **Mobile phones,** which, nowadays, are almost exclusively internet-enabled, have cameras, video recording functions and audio recorders built-in or these recording functions can be easily downloaded as apps.
  - **Personal cameras,** which often also record video footage as well as still images.
  - **Tablets**, e.g., iPads or Android tablets. These devices usually possess the features of mobile phones, outlined above.
  - **Laptops;** internet-enabled, have webcams and ability to record audio footage as well as video images.
  - **Smartwatches and wearable technology;** ability to access messages sent to mobile devices, some have the ability to record video and audio.

Why is there a safeguarding risk?

Whilst it is important that children and young people have photographs and films of special moments, the increasing use of digital technology presents a number of risks for children, young people, and their families, mainly due to the way it is used rather than the technology itself.

Safeguarding issues must be considered when taking and using images of children, young people, and staff, e.g., if they have fled from domestic abuse their whereabouts may be revealed to an abusive partner.

Some people simply do not want their images to be publicly available.

Prohibition of personal devices in education settings:

The use of Personal Devices whilst in contact with children **must be prohibited** for a number of reasons, e.g.

Distraction

- The focus for all adults in the setting should be on keeping children safe and ensuring their positive development.
- Having a personal device to hand means this is a distraction, and potential health and safety hazard.

Professional risk

- By using a personal device around children adults expose themselves to an increased professional risk of being accused of an inappropriate action, such as taking images of children.

Professional trust alone does not mitigate the safeguarding risk

- Leadership teams in education settings cannot control what personal devices are used for by the user.
- The use of personal devices in education settings when children are present is, in itself, an inappropriate act.
- Personal devices may not be used to take photographs or video images anywhere within the Settings grounds.

Personal Electronic Devices, Photographs and Images

Remember: It is both inappropriate and unnecessary to have a personal device to hand for any adult working with children, there is no reason to have access to a personal device until breaktimes and away from children

Developing the safeguarding culture and setting expectations around personal electronic devices

The use of personal devices should be part of the Code of Conduct at the setting.

Adults (Staff, Students and Volunteers) Should Never:

- Take photos of children in the setting where parents have not given their consent (the consent would be for the use of a professional device in all scenarios)
- Use a personal device, including wearable technology, to take photographs or store any personal information about a child or family.
- Comment about a child or their family on social media or other public forum
- Seek contact with or respond to requests for contact from a child or their family via personal phones, text, e-mail, or social networking accounts.
- Give their personal contact details to a child or parent including e-mail, social networking, home, or mobile phone numbers.

Please note: If a child attending the setting or their family is a personal friend or relative, the staff member, student or volunteer must inform their line manager at the earliest opportunity.

Suggestions for supporting staff with a change in safeguarding culture about personal electronic devices

Safe storage of personal devices

- It is acknowledged that personal devices are a part of everyday life for adults and that they are highly likely to be brought into the setting by an adult.
- Settings should designate the safe place for personal devices to be stored during work time, such as having secure lockers available for personal devices to be locked away.

Mobile/Personal Device Zones

- The location where personal devices can be used (Mobile Zones) should be defined in the setting, such as a staffroom/communal area for adults where children cannot and will not be present.

Clear Emergency Contact Procedure

- It is not appropriate for adults to be contacted via their personal devices during their working time in contact with children, as being directly alerted to a family emergency, for example, at this time could cause upset which is not appropriate for children to witness.
- Settings should have an emergency contact procedure for adults in the setting, so that if an adult needs to be contacted the person attempting to make contact does so by going through administrative staff or manager, who has access to a device owned by the setting that is used for professional communication purposes.

Personal Electronic Devices, Photographs and Images

Use of professional devices

It is standard practice that settings use devices, such as tablets and cameras, to capture images of children for educational purposes, etc. These 'professional' devices, purchased and maintained by the setting, are the only ones that should be used to take images of children, **with parental/carer consent.**

A setting should never ask an adult to use a personal device to take images and/or recordings for any reason. Any such request should be refused.

Professional devices used for taking images, recording and video should be stored on-site securely and be password protected. They should not be removed from the setting.

Ensure that asset registers are always up to date, so that adults and the devices they use can be easily linked

Sheffield Children Safeguarding Partnership model acceptable use policy summary

An 'acceptable use' agreement for the use of a professional device, which includes the expectations for use, is highly recommended. Acceptable use agreements are often part of the staff code of conduct.

- The information systems are the property of the setting, and it is a criminal offence to use a computer for a purpose not permitted by senior management.
- I will ensure that my information systems use will always be compatible with my professional role.
- This organisation's information systems may not be used for private purposes, without specific permission from the senior management.
- This organisation may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately whether in organisation, taken off the organisation premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children and young people's safety to the organisation's Online Safety Lead Officer or the Designated Safeguarding Lead
- I will ensure that any electronic communications with children and young people are compatible with my professional role.
- I will promote online safety with children and young people in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- The organisation may exercise its right to monitor the use of information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use may be taking place.
- If I, or another member of staff, breach this Information Systems Code of Conduct, action may result in disciplinary action.

Personal Electronic Devices, Photographs and Images

Photographic/image consent

All settings need a policy about taking and publishing images during events and activities and what actions you take to keep children safe.
This policy must be available and understood by pupils (as appropriate) parents, staff, and volunteers.

- You must get the informed, signed consent of everyone appearing in the photograph, video, and image, including staff and the parents and carers of pupils, before it is created.
- Young people may be able to give consent themselves if they are considered able to make an 'informed' choice.
- If you believe a young person is making an informed choice, always check with your DSL/D to see if there are safeguarding issues that the young people themselves are unaware of or may not have considered.
- No images of a looked after child should be created or used without prior written and signed consent from their social worker and Local Authority
- Never use full names or other personal details of the subject of any image you use as children may become vulnerable to grooming.
- Always be clear about the purpose and audience for the image.
- If you use images from another agency, you need to check that agency has obtained informed consent.
- Only use secure equipment provided by your setting to take, store, and download images – never use your personal devices.
- When an image is transferred to your workplace network they should be erased immediately from their initial storage location
- Be careful about using images of children in swimming costumes or other revealing clothing due to the potential for misuse of images.
- Always destroy images once consent has expired or the child or young person has left your setting.
- Never take images of a child's injury or an audio recording of a disclosure, even if requested by children's social care.
- Family members can take photos of their child in school activities. Photos taken for personal use by family members are not covered by the Data Protection Act.

The press;
The press are exempt from the Data Protection Act.
If you invite them to your premises or event you need to obtain prior consent from all staff, parents and carers involved.

Some key considerations;

CCTV and webcams:
- Are they sited where they may compromise the privacy of individuals, e.g., toilet or changing areas?
- Have you displayed clear signs that they are in operation?

Images:
- Are your display boards seen by the public?
- May be shared online, copied, downloaded, screenshotted, adapted and used inappropriately.
- May appear in internet search results.
- May become owned by the platform once posted and then licensed for e.g., commercial purposes.
- Become a part of a child's public image which may affect them later e.g., job applications.
- Have you demonstrated an inclusive approach by including images of people of different ethnicity or disability?

Personal Electronic Devices, Photographs and Images

- Have you checked any copyright implications?

Useful links

Data Protection: Gov.uk
SCSP Child Protection & Safeguarding Procedures: Online Safety
Safeguarding Sheffield Children website: Online Safety
Searching, screening and confiscation; Advice for Head Teachers, school staff & governing bodies, DfE 2018
Taking Photo's in Schools, Information Commissioners Office
Minimising Professional Risk
SCSP Online Safety key information